RANDOM NUMBER GENERATOR

Patent number:	JP61097746
Publication date:	1986-05-16
Inventor:	TEZUKA TSUDOI
Applicant:	IBM
Classification:	
- international:	G06F7/58; H03K3/84
- european:	G06F7/58P1
Application number:	JP19840214467 19841015
Priority number(s):	JP19840214467 19841015

Also published as:

EP0178432 (A:
US5046036 (A
EP0178432 (A:
EP0178432 (B:

Abstract not available for JP61097746
Abstract of corresponding document: **US5046036**

A pseudorandom number generator includes: an M-sequence generator having a plurality of stages ai; and a matrix product circuit which combines a matrix G having components gji with the stages ai to provide output elements bj of a number, each bj being represented by the expression, bj= SIGMA iajgji.

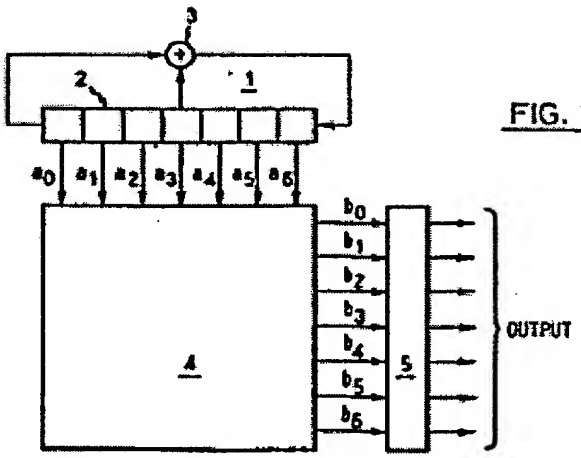


FIG. 1

⑲日本国特許庁（JP）　⑪特許出願公開

⑫公開特許公報（A）　昭61－97746

⑤Int.Cl.⁴	識別記号	庁内整理番号	㊸公開　昭和61年(1986)5月16日
G 06 F 7/58		7056－5B	
H 03 K 3/84		8425－5J	

審査請求　有　発明の数 1　（全11頁）

㊹発明の名称　乱数発生装置

㉑特　願　昭59－214467

㉒出　願　昭59(1984)10月15日

㉒発明者　手塚　集　東京都渋谷区恵比寿３－25－３　睦荘11号

㉑出願人　インターナショナル・ビジネス・マシーンズ・コーポレーション　アメリカ合衆国　10504　ニューヨーク州　アーモンク（番地なし）

㉔代理人　弁理士　澤田　俊夫　外２名

明　細　書

1．発明の名称　乱数発生装置

2．特許請求の範囲

(1)　フィードバックシフトレジスタを含んでなる多項式回路と、

上記フィードバックシフトレジスタから得られるパラレルなビットデータＡを受け取り

Ａ×Ｇ（ただしＡはベクトル、Ｇは行列である）の行列積を実行する手段とを有する乱数発生装置。

(2)　上記多項式回路をＭ系列発生器とした特許請求の範囲第１項記載の乱数発生装置。

(3)　ｋ次均等分布の乱数が生成されるように上記行列Ｇを選定した特許請求の範囲第２項記載の乱数発生装置。

(4)　漸近的乱数が生成されるように上記行列Ｇを選定した特許請求の範囲第３項記載の乱数発生装置。

3．発明の詳細な説明

〔産業上の利用分野〕

この発明はシフトレジスタ回路を利用した乱数発生装置に関し、とくに簡易な構成でありながら性質の良好な乱数を発生できるようにしたものである。

〔従来技術〕

近年Ｍ系列発生器（Maximum Length Shift Register Sequence Generator）を利用した一様乱数発生装置が着目されている。Ｍ系列発生器はその係数多項式をガロア体上の原始多項式に選んだものであり、出力される数列の周期を係数多項式が同一次数の範囲で最大にするものである。もちろんＭ系列発生器から発生される数列からその要素をどのように取り出して乱数に用いるかについては留意する必要がある。たとえばＭ系列$\{a_i\}$から$\{a_j, \cdots, a_{j+k}\}$、$\{a_{j+1}, \cdots, a_{j+k+1}\}$、$\{a_{j+2}, \cdots, a_{j+k+2}\}$というように乱数を選んでいくと、継続する乱数間に強い関連性が生じ不適切である。

Ｍ系列から一様乱数を発生させる主たる手法と

してはTausvortheの方法とLevis及びPayneの方法とが知られている。

Tausvorthe の方法では、M系列 $\{a_i\}$ の継続するg（≦p。ただしpは系数多項式の次数）個の要素の並べて、gビットの2進小数

$$V_i=0.a_{\sigma i+r-1}\ a_{\sigma i+r-2}\cdots a_{\sigma i+r-g}$$

を得、これを乱数とするものである。なおσはM系列から相続くg個の要素を取り出す間隔である。この手法の概要を第5図に示す。このように生成された乱数ではM系列の周期Tと間隔σとを互いに素に選ぶと (w_i) の周期もTとなり、またその一周期中には0が 2^{r-g} 回ずつ現われる。従つてpがgより十分大きければこの乱数は一様に分布することがわかる。

Levis及び Payne方法は特性方程式として

$$f(D)=D^p+D^q+1\quad(p>q)$$

を用い、これによつて生成されるM系列 (a_i) の位相を適当にずらしたものを並べて、2進小数

$$w_i=0.a_ia_{i+r_2}\cdots a_{i+r_g}$$

を得、これを乱数とするものである。この手法の概要を第6図に示す。この手法のM系列 (a_i) は漸化式

$$a_i=a_{i-p}+a_{i-q}\ (\mathrm{mod}\ 2)$$

を満たし、この結果 $\{w_i\}$ は漸化式

$$w_i=w_{i-p}\oplus w_{i-q}$$

で生成できる。ただし⊕はビットごとの排他的論理和である。

しかしながら上述2つの手法には重大な欠点がある。即ちTausvortheの方法では乱数発生に要する時間が長くなつてしまう。またLevis及びPayneの方法では一様性が不明となる欠点がある。この方法自体からは乱数の一様性が保証されていず、そのため一様性があるのかないのかを吟味する必要がある。

［発明が解決しようとする問題点］

この発明は以上の事情を考慮してなされたものであり、M系列発生器等のシフトレジスタ回路から出力される数列をシャッフリングして出力する乱数発生装置であつて、その構成から乱数の性質を知ることができ、このためその性質についての吟味をする必要がなく、かつ乱数発生の所要時間が短かいものを提供することを目的としている。

この発明はより具体的にはM系列発生器を利用して性質のすぐれた乱数を簡易に生成する乱数発生装置を提供することを目的としている。

［問題点を解決するための手段］

この発明は以上の目的を達成するために、“1”及び“0”を要素とする数列を発生するシフトレジスタ回路と、このシフトレジスタ回路からのパラレルな出力Aを受取りA×Gの行列積を実行する行列積回路とを有している。ただし、Aはベクトル、Gは行列である。

［実施例］

以下この発明の一実施例について説明しよう。

第1図はこの実施例を示すものであり、この図においてシフトレジスタ回路1は7ステージのシフトレジスタ2及びエクスクルーシブ・オア回路3からなつている。このシフトレジスタ回路1の特性方程式は $f(D)=D^7+D^6+1$ である。シフトレジスタ回路1は明らかにM系列発生器であり、2^7-1 の周期を有する。

シフトレジスタ2の各ステージからの出力は行列積回路4にパラレルに供給されている。この行列積回路4は行列G

$$G=\begin{bmatrix}1&0&0&0&0&0&0\\0&1&1&1&1&0&1\\0&1&1&0&0&1&1\\1&1&0&0&0&1&1\\1&1&1&1&0&1&0\\0&1&0&1&1&0&0\\1&1&1&0&1&1&1\end{bmatrix}$$

で表わすことができる。シストレジスタ2の各ステージからの出力の成分を a_i ($i=0\sim6$) とすれば行列積回路4の出力 b_j ($j=0\sim6$) は $b_j=\sum_i a_i g_{ji} \pmod 2$ である。ただし、g_{ji} は行列Gの成分である。行列積回路の出力は一旦ラッチ5にラッチされたのち2進小数乱数w

$$w=0.b_0b_1\cdots b_6$$

として出力される。

なお行列積回路4は例えば第2図に示すように構成することができる。この図において6はエクスクルーシブ・オア回路、7は行信号線、8は列信号線である。

この乱数発生装置から発生する乱数の性質を理解するために2次元での分布を求めた。これを第3図に示す。2次元の分布とは継続する乱数(w_i, w_{i+1})の分布を調べたものである。図に示す分布には規則性がなく、かつ一様性があることが明らかである。このことは継続する2つの乱数の関連性がなく、しかも乱数の発生確率が特定のものにかたよらないことを意味する。この乱数発生装置の乱数がすぐれた性質を有することがわかる。このことの詳細はのちに理解される。つぎに行列Gの意味について考察を加えることにする。

結論から言えば行列Gによつて生成される乱数は7ビットの漸近的なLewis及びPayneの乱数である。漸近的乱数(asymptotically random number)の意味はのちに理解される。

まずk次均等分布(k-distribution)の概念を導入しよう。この概念は乱数の一様性の目安となるものである。

定義

乱数 $\{w_i\}$ の継続するk個の要素を座標成分とする点を x_i とするとき、k次元超立方体内の任意の点x(座標成分がlビットの2進小数で表わせるもの)に対して $p(x_i=x)=2^{-kl}$ が成立するとき乱数 $\{w_i\}$ はk次均等分布をするという。ここで確率pは1周期全体にわたる相対頻度を意味する。

座標成分がlビットで、次元がkであるから超立方体内の点は 2^{lk} 個である。$p(x_i=x)=2^{-kl}$ であれば乱数 $\{w_i\}$ が各点xに均等に分布することは明らかである。

M系列に基づく系列 $\{w_i\}$ の分布に即して言えば、k次均等分布をつぎのように言うことができる。

定義

$(w_i, w_{i+1}, \cdots, w_{i+k-1})$ をkl組と見なすとき、1周期にすべての成分が0の組は $2^{p-kl}-1$ 回、他のすべてのパターンはいずれも 2^{p-kl} 回出現するならば、(w_i) はk次均等分布をする(このことから $p\leq kl$ であることは明らかである)。

k個の継続する乱数を用いてシミュレーションを行うときk次均等分布が肝要となることは明らかであろう。

さてLewis及びPayneの乱数がk次均等分布であるためには、乱数 w_i を

$$w_i=0.a_{jl+1}a_{jl+2}\cdots a_{jl+l}$$

とし、$k=\lfloor p/l \rfloor$ として、次の行列 $\hat{G}$ の各行ベクトルが線形独立になることが、必要十分である(このことについてはCommunications of the ACM Vol.26, pp516-523を参照されたい)。

$$\begin{bmatrix} A_{j1} \\ \cdot \\ \cdot \\ \cdot \\ A_{j1+k-1} \\ A_{j2} \\ \cdot \\ \cdot \\ \cdot \\ A_{j2+k-1} \\ \cdot \\ \cdot \\ \cdot \\ A_{j\ell} \\ \cdot \\ \cdot \\ \cdot \\ A_{j\ell+k-1} \end{bmatrix} = \begin{bmatrix} \\ \hat{G} \\ \\ \\ (\hat{G}\text{は}\ \ell \cdot k\text{行}, p\text{列}) \end{bmatrix} \cdot \begin{bmatrix} A_1 \\ A_2 \\ \cdot \\ \cdot \\ \cdot \\ A_i \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ A_p \end{bmatrix}$$

ただし (a_i) はM系列、pはM系列の特性方程式の次数、$\lfloor p/\ell \rfloor$ は p/ℓ を超えない最大の整数、A_i は $(a_i\ a_{i+1}\cdots)$ である。

このことを $p=7$, $\ell=7$ の乱数に適用する。まず $k=\lfloor 1/1 \rfloor=1$ である。そして

$$\begin{bmatrix} A_{j1} \\ A_{j2} \\ A_{j3} \\ A_{j4} \\ A_{j5} \\ A_{j6} \\ A_{j7} \end{bmatrix} = \begin{bmatrix} \hat{G}_7 \\ \cdot \end{bmatrix} \cdot \begin{bmatrix} A_1 \\ A_2 \\ A_3 \\ A_4 \\ A_5 \\ A_6 \\ A_7 \end{bmatrix}$$

を満たす $\hat{G}_7$ の行ベクトルが線形独立であればよい。なお $\hat{G}_7$ のサフイツクス7は $\ell=7$ であることを示す。

他方第1図の実施例の乱数は

$$\begin{bmatrix} A_{j1} \\ A_{j2} \\ A_{j3} \\ A_{j4} \\ A_{j5} \\ A_{j6} \\ A_{j7} \end{bmatrix} = \begin{bmatrix} 1000000 \\ 0111001 \\ 0110011 \\ 1100011 \\ 1111010 \\ 0101100 \\ 1110111 \end{bmatrix} \cdot \begin{bmatrix} A_1 \\ A_2 \\ A_3 \\ A_4 \\ A_5 \\ A_6 \\ A_7 \end{bmatrix}$$

で表わすことができる。この式において行列Gの行ベクトルが線形独立なことは明らかである。このことから行列式回路4から出力される乱数 $(a_{J_1}\ a_{J_2}\cdots a_{J_7})$, $(a_{J_2+1}\ a_{J_2+1}\cdots a_{J_7+1})$ が7ビット1次均等分布をするLevis及びPayneの乱数であることがわかる。

次に、漸近的乱数との関連でこの実施例の乱数について考察する。

一般にモンテカルロ法等のシミュレーションのために乱数を使用するとき、要求される精度（ビット長）はその目的によりさまざまである。従つて任意のビット長に対しk次均等分布が保証されていることが望ましい。例えば $p=7$ のときの数列 a_{J_1+1}, a_{J_2+1}, $a_{J_3+1}\cdots$ を考えよう。そしてこの数列のうち上位7ビットを乱数としたときには1次均等分布（$k=\lfloor 7/7 \rfloor=1$）が確立されているけれども、上位3ビットを乱数としたときには2次均等分布（$k=\lfloor 7/3 \rfloor=2$）が確立されていないとしよう。そうすると、この数列から $\ell=7$ の乱数を取り出すことは好ましいが、$\ell=3$ の乱数を取り出すことは不適切となつてしまう。このことは不都合である。

漸近的乱数は以上の不都合が解消されている乱数である。これはつぎのようにいうことができる。

定義

次の2条件を満たすLevis及びPayneの乱数を漸近的にランダムなsビットのLevis及びPayneの乱数と呼ぶ。

条件1：行列 $\hat{G}_s$ の行ベクトルが任意の ℓ $(\leq s)$ に対して線形独立となる。

条件2：周期が素数となる；

なお、条件2はつぎのような要請に応えるものである。即ち通常k次元のシミュレーションで乱

数を使用する場合一様乱数 w_i のオーバーラップしない k 組（$w_{k\ell}$, $w_{k\ell+1}$, ・・・・ $w_{k\ell+k-1}$）を用いる。条件2はこの列に対してk均等分布を保証するために必要となる。

さて、第1図の実施例で発生させられる乱数が漸近的乱数かどうかについて考えよう。まず $\ell=7$ の場合には $k=1$ であり、

$$\begin{bmatrix} A_{j1} \\ A_{j2} \\ A_{j3} \\ A_{j4} \\ A_{j5} \\ A_{j6} \\ A_{j7} \end{bmatrix} = \begin{bmatrix} 1000000 \\ 0111001 \\ 0110011 \\ 1100011 \\ 1111010 \\ 0101100 \\ 1110111 \end{bmatrix} \cdot \begin{bmatrix} A_1 \\ A_2 \\ A_3 \\ A_4 \\ A_5 \\ A_6 \\ A_7 \end{bmatrix}$$

が成立しているので1次的等分布が確立していることは明らかである。

$\ell=4$，5及び6の場合には、$k=1$ でありそれぞれ上述から

$$\begin{bmatrix} A_{j1} \\ A_{j2} \\ A_{j3} \\ A_{j4} \\ A_{j5} \\ A_{j6} \end{bmatrix} = \begin{bmatrix} 1000000 \\ 0111001 \\ 0110011 \\ 1100011 \\ 1111010 \\ 0101100 \end{bmatrix} \cdot \begin{bmatrix} A_1 \\ A_2 \\ A_3 \\ A_4 \\ A_5 \\ A_6 \\ A_7 \end{bmatrix}$$

が導き出され、これらの式から $\ell=4$，5及び6の場合に一次均等分布が確立されることは明らかである。

$\ell=3$ の場合には $k=\lfloor 7/3 \rfloor = 2$ であり、また上述 $\hat{G}_7$ から

$$\begin{bmatrix} A_{j1} \\ A_{j2} \\ A_{j3} \\ A_{j4} \\ A_{j5} \\ A_{j6} \\ A_{j7} \end{bmatrix} = \begin{bmatrix} 1000000 \\ 0111001 \\ 0110011 \\ 1100011 \\ 1111010 \\ 0101100 \end{bmatrix} \cdot \begin{bmatrix} A_1 \\ A_2 \\ A_3 \\ A_4 \\ A_5 \\ A_6 \\ A_7 \end{bmatrix}$$

$$\begin{bmatrix} A_{j1} \\ A_{j2} \\ A_{j3} \\ A_{j4} \\ A_{j5} \end{bmatrix} = \begin{bmatrix} 1000000 \\ 0111001 \\ 0110011 \\ 1100011 \\ 1111010 \end{bmatrix} \cdot \begin{bmatrix} A_1 \\ A_2 \\ A_3 \\ A_4 \\ A_5 \\ A_6 \\ A_7 \end{bmatrix}$$

$$\begin{bmatrix} A_{j1} \\ A_{j1+1} \\ A_{j2} \\ A_{j2+1} \\ A_{j3} \\ A_{j3+1} \end{bmatrix} = \begin{bmatrix} 1000000 \\ \hline 0111001 \\ \hline 0110011 \\ \hline \end{bmatrix} \cdot \begin{bmatrix} A_1 \\ A_2 \\ A_3 \\ A_4 \\ A_5 \\ A_6 \\ A_7 \end{bmatrix}$$

が導き出される。ここで横棒で表わした第2、第4及び第6の行ベクトルがそれぞれ第1、第3及び第5の行ベクトルから一意的に決定されることに留意されたい。結論から述べよう。第1、第3第5の行ベクトルのうち任意のものを $\overline{g}_j$ で表わし、第2、第4及び第6の行ベクトルのうち対応するものを $\overline{g}_{j+1}$ で表わし、さらに $\overline{g}$ を（g_1, g_2, g_3, ・・・・, g_7）で表記するとしよう。

$\overline{g}_{j+1}$ は次のようにして $\overline{g}_j$ から求まる。

$$g_{j+1,1}=g_{j,7}$$
$$g_{j+1,2}=g_{j,1}$$
$$g_{j+1,3}=g_{j,2}$$
$$g_{j+1,4}=g_{j,3}+g_{j,7}$$
$$g_{j+1,5}=g_{j,4}$$
$$g_{j+1,6}=g_{j,5}$$
$$g_{j+1,7}=g_{j,6}$$

例えば第3行の行ベクトル$\overline{g}_{j_2}$＝（0111001）であるから第4行の行ベクトル$\overline{g}_{j_2+1}$＝（1010100）となる。同様にして第2行及び第6行の行ベクトルも求め、つぎの行列$\hat{G}_3$を得る。

$$\hat{G}_3=\begin{bmatrix}1&0&0&0&0&0&0\\0&1&0&0&0&0&0\\0&1&1&1&0&0&1\\1&0&1&0&1&0&0\\0&1&1&0&0&1&1\\1&0&1&0&0&0&1\end{bmatrix}$$

この行列G_3の各行ベクトルは線形独立となつているので、この実施例の乱数は$q=3$の場合に2次均等分布となることがわかる。

さて行ベクトル$\overline{g}_{j+1}$が行ベクトル$\overline{g}_j$から一意的に決定されることについて考えておく。

既述のとおり$q=3$、$k=2$ではつぎの式が成立する。

$$\begin{bmatrix}A_{j1}\\A_{j1+1}\\A_{j2}\\A_{j2+1}\\A_{j3}\\A_{j3+1}\end{bmatrix}=\begin{bmatrix}\hat{G}_3\end{bmatrix}\cdot\begin{bmatrix}A_1\\A_2\\A_3\\A_4\\A_5\\A_6\\A_7\end{bmatrix}$$

この式からA_j（A_{j_1}，A_{j_2}またはA_{j_3}）は

$$A_j=g_{j,1}\cdot A_1+g_{j,2}\cdot A_2+g_{j,3}\cdot A_3+g_{j,4}\cdot A_4+g_{j,5}\cdot A_5+g_{j,6}\cdot A_6+g_{j,7}\cdot A_7$$

である。また上の式で数列Aの位相を1つずらすと、

$$\begin{bmatrix}A_{j1+1}\\A_{j1+2}\\A_{j2+1}\\A_{j2+2}\\A_{j3+1}\\A_{j3+2}\end{bmatrix}=\begin{bmatrix}\hat{G}_3\end{bmatrix}\cdots\begin{bmatrix}A_2\\A_3\\A_4\\A_5\\A_6\\A_7\\A_8\end{bmatrix}$$

を得るのでA_{j+1}は

$$A_{j+1}=g_{j,1}\cdot A_2+g_{j,2}\cdot A_3+g_{j,3}\cdot A_4+g_{j,4}\cdot A_5+g_{j,5}\cdot A_6+g_{j,6}\cdot A_7+g_{j,7}\cdot A_8$$

である。

ところでLevis及びPhayneの数列$\{a_i\}$（ただし$f(D)=D^7+D^3+1$）では$a_i=a_{i-3}+a_{i-7}$が成立するので$A_8=A_5+A_1$である。従つてA_{j+1}

はつぎのように整理される。

$$A_{j+2}=g_{j+7}\cdot A_1+g_{j+6}\cdot A_2+g_{j+5}\cdot A_3+(g_{j+4}+g_{j+7})\cdot A_4+g_{j+3}\cdot A_5+g_{j+2}\cdot A_6+g_{j+1}\cdot A_7$$

$\overline{g}_j$から$\overline{g}_{j+1}$を求め得ることは以上から理解できる。

なおここではg_{j+1}とg_jとについて述べたが$\overline{g}_{j+2}$, g_{j+3}……をそれぞれ$\overline{g}_{j+1}$, $\overline{g}_{j+2}$……から求めることができることももちろんである。このことの証明は上述と同様であり、繰り返さない。

さてこの実施例の漸近的ランダムネスの考察に戻ろう。$\ell=2$の場合には$k=\lfloor 7/2 \rfloor=3$であり、また$\hat{G}_1$及び$\hat{G}_2$から

$$\begin{bmatrix} A_{j1} \\ A_{j1+1} \\ A_{j1+2} \\ A_{j2} \\ A_{j2+1} \\ A_{j2+2} \end{bmatrix} = \begin{bmatrix} 1\,0\,0\,0\,0\,0\,0 \\ 0\,1\,0\,0\,0\,0\,0 \\ \hline 0\,1\,1\,1\,0\,0\,1 \\ 1\,0\,1\,0\,1\,0\,0 \\ \hline \end{bmatrix} \cdot \begin{bmatrix} A_1 \\ A_2 \\ A_3 \\ A_4 \\ A_5 \\ A_6 \\ A_7 \end{bmatrix}$$

が導き出される。この場合も横棒で示す行ベクトルをそれぞれ直ぐ上の行ベクトルから決定して

$$\hat{G}_2 = \begin{bmatrix} 1\,0\,0\,0\,0\,0\,0 \\ 0\,1\,0\,0\,0\,0\,0 \\ 0\,0\,1\,0\,0\,0\,0 \\ 0\,1\,1\,1\,0\,0\,1 \\ 1\,0\,1\,0\,1\,0\,0 \\ 0\,1\,0\,1\,0\,1\,0 \end{bmatrix}$$

を得る。各行ベクトルは線形独立なので3次均等分布が確立することがわかる。

$\ell=1$の場合には$k=\lfloor 7/1 \rfloor=7$であり、また$\hat{G}_1$, $\hat{G}_2$及び$\hat{G}_3$から

$$\begin{bmatrix} A_{j1} \\ A_{j1+1} \\ A_{j1+2} \\ A_{j1+4} \\ A_{j1+5} \\ A_{j1+6} \end{bmatrix} = \begin{bmatrix} 1\,0\,0\,0\,0\,0\,0 \\ 0\,1\,0\,0\,0\,0\,0 \\ 0\,0\,1\,0\,0\,0\,0 \\ \hline \\ \hline \\ \hline \end{bmatrix} \cdot \begin{bmatrix} A_1 \\ A_2 \\ A_3 \\ A_4 \\ A_5 \\ A_6 \\ A_7 \end{bmatrix}$$

が導き出される。この場合も横棒で示す行ベクトルをそれぞれ直ぐ上の行ベクトルから順次決定して

$$\hat{G}_3 = \begin{bmatrix} 1\,0\,0\,0\,0\,0\,0 \\ 0\,1\,0\,0\,0\,0\,0 \\ 0\,0\,1\,0\,0\,0\,0 \\ 0\,0\,0\,1\,0\,0\,0 \\ 0\,0\,0\,0\,1\,0\,0 \\ 0\,0\,0\,0\,0\,1\,0 \\ 0\,0\,0\,0\,0\,0\,1 \end{bmatrix}$$

を得る。各行ベクトルは線形独立なので7次均等分布が確立することがわかる。

以上からこの実施例の乱数が7ビット漸近的な乱数であることがわかる。

なお、第4図はこの実施例の乱数の上位3ビットを使つた場合の2次均等分布の状態を示している。これに対し、第3図は下位の4ビットも含めた全ビットを使用した場合の2次元分布の状態を示している。第3図から下位4ビットによつて2次元分布の規則性を解消していることがわかる。このような規則性の解消は下位4ビットに対応する、行列Gの第4～7の行ベクトルからなる行列のランクを高くすることにより達成される。

つぎに実施例の行列Gの決定のしかたについて述べる。7ビット漸近的な乱数を発生させるためには$\ell=1$から7まで順にk次均等分布を確立するように行ベクトルを決定していけばよい。

$\ell=1$

まず行列$\hat{G}_1$の任意の1つの行ベクトルを設定する。上述から理解されるように他の行ベクトル

は一意的に決定される。つぎにこのようにして得た行列$\hat{G}_1$の各行ベクトルが線形独立になつているかどうかを調べる。線形独立になつていれば、この行列$\hat{G}_1$を正規のものとして選ぶ。線形独立になつていなければ最初に設定する行ベクトルを他のものにして同様の操作を行う。

例えば行列$\hat{G}_1$の第1行ベクトルを（1000000）とすると行列G_1はつぎのようになる。

$$\hat{G}_1 = \begin{bmatrix} 1000000 \\ 0100000 \\ 0010000 \\ 0001000 \\ 0000100 \\ 0000010 \\ 0000001 \end{bmatrix}$$

この行列$\hat{G}_1$の各行ベクトルは線形独立であるのでこれを正規のものとして選ぶことができる。この選択により$\ell = 1$のときの7次均等分布が保証される。

$\ell = 2$

行列$\hat{G}_2$の第1、第2及び第3行の行ベクトルは行列$\hat{G}_1$の第1、第2及び第3行の行ベクトルと同一であり、

$$\hat{G}_2 = \begin{bmatrix} 1000000 \\ 0100000 \\ 0010000 \\ \hline \\ \hline \\ \hline \end{bmatrix}$$

である。横棒で示す未決定の行ベクトルは$\ell = 1$の場合と同様に求める。即ち、得られる行列$\hat{G}_2$の各行ベクトルが線形独立になるように、未決定の行ベクトルのうち任意の1つを設定する。

例えば第4行の行ベクトルを（0111001）とすると行列$\hat{G}_2$としてつぎのものが得られる。

$$\hat{G}_2 = \begin{bmatrix} 1000000 \\ 0100000 \\ 0010000 \\ 0111001 \\ 1010100 \\ 0101010 \end{bmatrix}$$

この行列$\hat{G}_2$の各行ベクトルは線形独立であるのでこれを正規のものとして選ぶことができる。この選択により$\ell = 2$のときの3次均等分布が保証される。

$\ell = 3$

行列$\hat{G}_3$の第1、第2、第3及び第4の行ベクトルは行列$\hat{G}_2$の第1、第2、第4及び第5の行ベクトルと同一であり、

$$\hat{G}_3 = \begin{bmatrix} 1000000 \\ 0100000 \\ 0111001 \\ 1010100 \\ \hline \\ \hline \end{bmatrix}$$

である。この場合も上述と同様に第5行及び第6行の行ベクトルを適切に選定して2次均等分布を満たす行列$\hat{G}_3$を得る。

例えば行列G_3はつぎのようなものである。

$$\hat{G}_3 = \begin{bmatrix} 1000000 \\ 0100000 \\ 0111001 \\ 1010100 \\ 0110011 \\ 1010001 \end{bmatrix}$$

$s=4, 5, 6$及び7

$s=4, 5, 6$及び7の場合にも同様にして行列$\hat{G}_4$、$\hat{G}_5$、$\hat{G}_6$及び$\hat{G}_7$のうち未決定の行ベクトルを決定していく。以下はそのようにして得た行列G_4、G_5、G_6及びG_7の一例である。ただしアンダーラインは新たく設定した行ベクトルを示す。

$$\hat{G}_4 = \begin{bmatrix} 1000000 \\ 0111001 \\ 0110011 \\ \underline{1100011} \end{bmatrix}$$

$$\hat{G}_5 = \begin{bmatrix} 1000000 \\ 0111001 \\ 0110011 \\ 1100011 \\ \underline{1111010} \end{bmatrix}$$

$$\hat{G}_6 = \begin{bmatrix} 1000000 \\ 0111001 \\ 0110011 \\ 1100011 \\ 1111010 \\ \underline{0101100} \end{bmatrix}$$

$$\hat{G}_7 = \begin{bmatrix} 1000000 \\ 0111001 \\ 0110011 \\ 1100011 \\ 1111010 \\ 0101100 \\ \underline{1110111} \end{bmatrix}$$

このような行列$\hat{G}_4$, $\hat{G}_5$, $\hat{G}_6$及び$\hat{G}_7$は一次均等分布を保証する。

行列$\hat{G}_7$が行列積回路4の行列Gとして用いられることは既に述べた。行列積回路4の出力の上位1ビットを用いると7次均等分布の乱数が得られ、上位2ビット、3ビットをそれぞれ用いて3次、4次均等分布の乱数が得られることについては説明を要しないであろう。

なお、この発明は上述実施例の構成の細部に拘束されないことはもちろんである。

例えば上述では7ビット漸近的な乱数を発生するようにしたけれどもビット数は適切に選定することができる。例えば31ビット漸近的な乱数をつぎの行列を実現する行列積回路により生成するようにしてもよい。なお特性方程式は$f(D) = D^{31} + D^{28} + 1$である。

$$G = \begin{bmatrix}
1000000000000000000000000000000 \\
1001001000001011101011000010011 \\
0110101101011001001111010000101 \\
0100010011101001110000000000000 \\
0010101111001000110000000000000 \\
1000100011010100100011111001010 \\
0001110010110000010000000000000 \\
0110010110000011010100000101011 \\
0101100010110000011100100010001 \\
0111111100010010011111000000011 \\
0010001111010111000110101100001 \\
1111011011001101011110110100000 \\
1000010100001100001010110101011 \\
0101000001111011011000110000100 \\
0000010011010110110110000000111 \\
0111001011000001000000000000000 \\
0100011110101110001101011000010 \\
1101110110011010111101101000001 \\
0010101000011000010101101010111 \\
1011000011110110110001100001000 \\
0000100110101101101100000001110 \\
0000110110111000110100000011000 \\
1010111111001000010100111011010 \\
1111000101111010011001111011010 \\
1100100100010000000100101111011 \\
0000110010001100101101000100011 \\
1100001010001111000011111010000 \\
1000100010100100001011101001010 \\
1111000010111011001011001111000 \\
1110010001001110000010111101010 \\
0001010101001001001110001000100
\end{bmatrix}$$

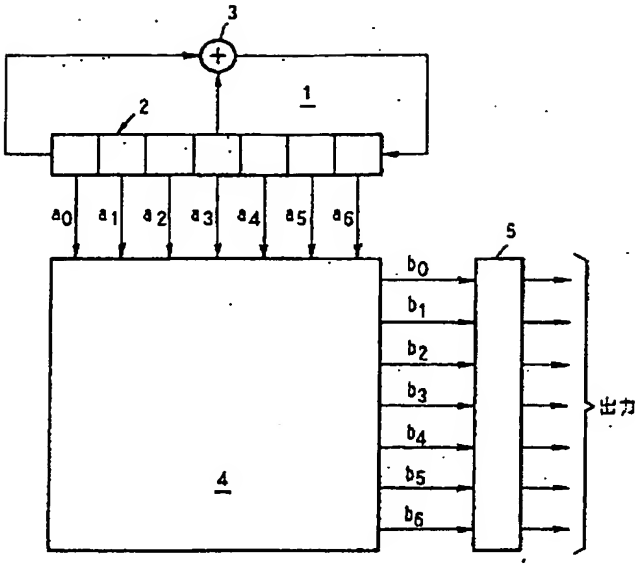
〔発明の効果〕

以上説明したようにこの発明によればシフトレジスタ回路の出力を行列積回路に供給してシャッフリングするようにしている。従つて乱数の発生の所要時間を短かくすることができる。また、行列積回路の行列から乱数の性質を知ることができ、あらためてその性質を吟味する必要がない。

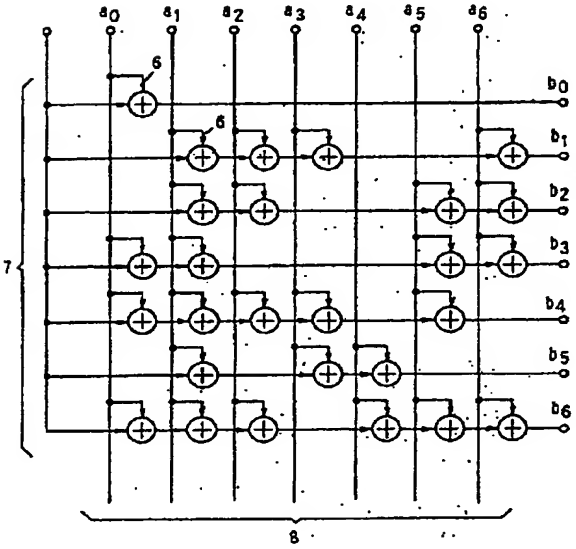
また行列積回路の行列を適切に選ぶことによりsビット漸近的な乱数を簡易に生成することができる。

4．図面の簡単な説明

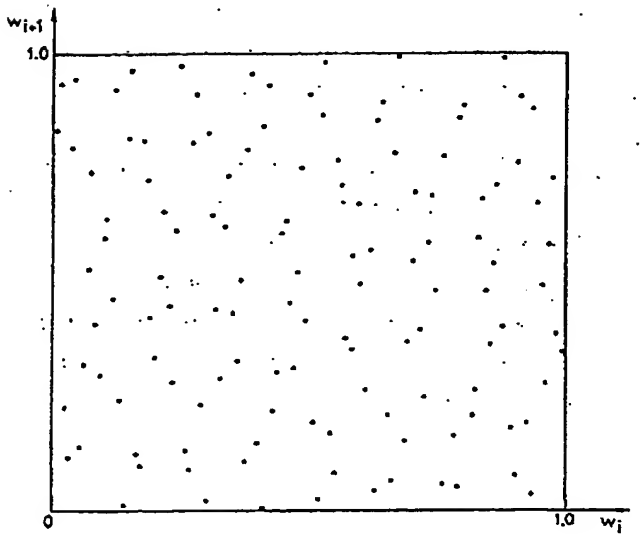
第1図はこの発明の一実施例を示すブロック図、第2図は第1図の行列積回路4の構成例を示す回路図、第3図及び第4図は第1図実施例を説明するための図、第5図及び第6図はそれぞれTausworthの方法及びLewis Payneの方法を説明する図である。



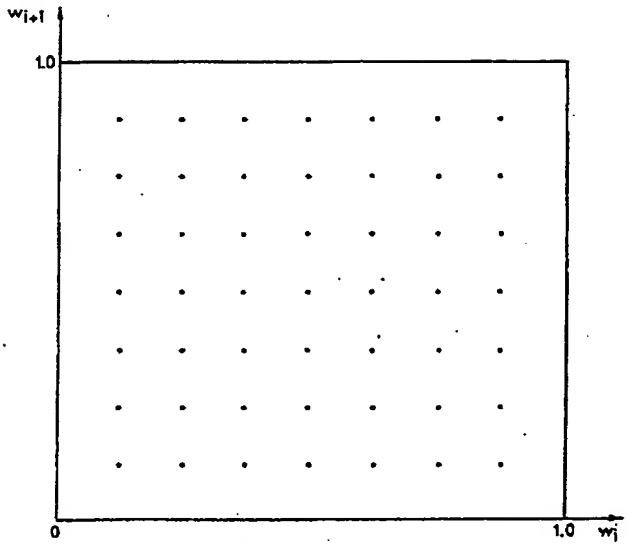
第1図



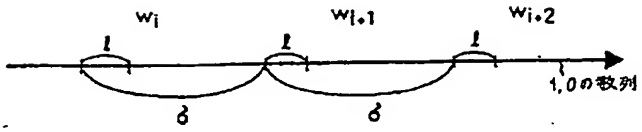
第2図



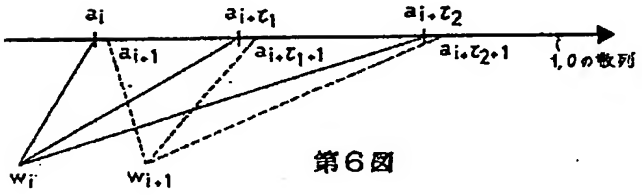
第3図


wi+1
1.0
0
1.0
wi

第4図


wi
wi+1
wi+2
1
1
1
δ
δ
1,0の数列

第5図


ai
ai+τ1
ai+τ2
ai+1
ai+τ1+1
ai+τ2+1
1,0の数列
wi
wi+1

第6図